

**Annual 47 C.F.R. Section 64.2009(e) CPNI Certification**  
**EB Docket 06-36**

Annual 64 2009(e) CPNI Certification for **2007**

Date Filed: **February 22, 2008**

Name of company covered by this certification: **Cordova Telephone Cooperative, Inc**

Form 499 Filer ID: **806772**

Name of signatory: **Paul Kelly**

Title of signatory: **CEO-GM**

I, Paul Kelly, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules *See 47 C.F.R. Section 64.2001 et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules [attach accompanying statement]

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI  
If affirmative: [provide explanation of any actions taken against data brokers]

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.* instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).  
If affirmative: [provide summary of all customer complaints received in the past year concerning the unauthorized release of CPNI]

Signed  [electronic signature if applicable]

OPERATING PROCEDURES FOR COMPLIANCE  
WITH CPNI REGULATIONS

Every employee of CORDOVA TELEPHONE COOPERATIVE (the "Company") has a duty to protect the confidentiality of customer proprietary information ("CPNI"), as defined in 47 U.S.C. § 222(f). A violation of the Company's operating procedures will result in disciplinary action. For a first violation, an employee will be given a warning and the violation will be noted on the employee's record. An employee will be subject to termination of employment for a second violation.

The service categories provided by the company include local exchange telephone service and Internet access service. It is the Company's policy to not use CPNI for any sales or marketing purpose. Specifically, use of CPNI obtained from the Company's provision of one service category to market a second service category to individuals or businesses that are not already customers of that second service category is strictly prohibited.

No Company employee shall disclose CPNI to any Company affiliate or other third party unless such disclosure is required by a lawful subpoena or is used for the following purposes: (1) to bill or collect payment for the Company's services or (2) to protect the rights or property of the Company or its customers. A Company employee that receives or obtains CPNI for the purpose of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for any marketing purpose.

A Company employee shall disclose CPNI only upon an affirmative request by the customer and only after validating that the person requesting the information is the person that opened the account with the Company. The validation process must, at a minimum, include asking the person requesting CPNI for the last four digits of the customer's social security number and only disclosing the CPNI if the correct four digits are provided. No Company

employee shall disclose CPNI to a person other than the customer unless the customer provides written authorization affirmatively requesting that the customer's CPNI be disclosed to that person

The Company keeps a record of all instances where CPNI is disclosed or provided to third parties, or where third parties are allowed access to CPNI (hereinafter referred to as "the CPNI record"). An employee that discloses CPNI to a third party or allows a third party access to CPNI must add to the CPNI record the name and address of the third party, a description of the reasons for the disclosure of the CPNI, the specific CPNI that was disclosed, and any written authorization from the customer to disclose the CPNI. This record is maintained by the Company for a minimum period of one year.

The Company holds training sessions twice each month to train employees as to when they are and are not authorized to use or disclose CPNI. Employee attendance at these training sessions is mandatory.

Should the Company make a decision to modify its prohibition on the use of CPNI for marketing purposes, it will notify all employees of any such modifications. Under no circumstances will CPNI be used for any marketing purpose until after the Company has sent customers the notices required by 47 C.F.R. § 64.2008 and received the customer opt-in or opt-out approvals required for such use of CPNI. Sales personnel must obtain written supervisory approval before soliciting customer approval for any out-bound marketing campaign. The Company will establish a system by which the status of a customer's CPNI approval can be clearly established if the Company changes its current policy and decides to use CPNI in an out-bound sales or marketing campaign. Upon such a change in Company policy, employees must add to the CPNI record a description of each such out-bound marketing campaign, the specific

CPNI that was used in the campaign, and what products and services were offered as part of the campaign.

# **Customer Proprietary Network Information (CPNI)**

## **Operating Procedure for CPNI Rules and Compliance Procedures**

### **Purpose**

1. To ensure compliance with the FCC's CPNI rules (47 CFR 64.2001-64.2011) per Section 222 of the Communications Act of 1934, as amended
2. To outline the procedures required to protect the confidentiality of customer information
3. Procedures for use of CPNI to market enhanced or new services
4. Procedures for use of CPNI for handling customer requests
5. Annual review of CPNI policies and procedures with all employees and immediately upon hire of new employees
6. Annually file CPNI compliance filings with the FCC
7. Definitions related to FCC CPNI rules as contained in Part 64.2003

### **Customer Notification**

1. Cordova Telephone Cooperative (CTC) will notify and inform each Customer of his or her right to restrict the use or disclosure of, and access to, CPNI
2. CTC will maintain records of that notification, whether oral or written, for at least one year
3. The notification will provide information sufficient to enable our Customers to make informed decisions as to whether to permit the use or disclosure of, or access to, their CPNI
4. The notice will contain a statement that the Customer has a right, and we have a duty, under federal law, to protect the confidentiality of their CPNI
5. The notice will specify the types of information that constitute CPNI, the specific entities that will receive CPNI, describe the purposes for which the CPNI will be used, inform the Customer of his or her right to approve or disapprove those uses and to deny or withdraw access to CPNI use at any time. The Customer's approval, or disapproval, will remain in effect until the Customer affirmatively revokes or limits such approval or denial
6. CTC will advise the Customer of the precise steps the Customer must take in order to grant or deny access to CPNI and clearly state that a denial of approval will not affect the provision of any services to which the Customer subscribes
7. The statement will be in a clear and neutral language, which describes the consequences directly resulting from the lack of access to CPNI. In addition, we may state that the Customer's consent to use his or her CPNI may enhance our ability to offer products and services tailored to meet the Customer's needs and that we will disclose the Customer's CPNI to any person upon the affirmative written request of the Customer
8. For non-English speaking customers, should portions of a notice be translated into another language, then all portions of the notice are translated into that language
9. The notification will not include any statement that attempts to encourage a Customer to freeze third-party access to CPNI
10. New Customers will be verbally notified at the time of the request for service
11. In addition, a CPNI statement will be included in our new customer Welcome Packets

### **Use of CPNI**

1. CTC will use, disclose or permit access to CPNI to protect our rights, property, Customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, our services
2. CTC will use, disclose or permit access to CPNI to provide or market service offerings among the different categories of service – local, interexchange, etc. to which the Customer already subscribes
3. When CTC provides different categories of service, and a Customer subscribes to more than one service category, we may share the Customer's CPNI with the affiliate that provides service to the Customer; but if a Customer subscribes to only one service category, we do not share the Customer's CPNI with an affiliate without the Customer's approval
4. We use, disclose or permit access to CPNI derived from our provision of local exchange or interexchange service for the provision of CPE and call answering, voice mail or messaging, voice storage and retrieval services, and protocol conversion, without Customer approval
5. Without Customer approval, we do not use, disclose or permit access to CPNI to provide or market service offerings within a category of service to which the Customer does not already subscribe, except that we use, disclose or permit access to CPNI to do the following:
  - A. Provide inside wiring installation, maintenance and repair services
  - B. Services such as, but not limited to, speed dialing, computer-provided directory assistance, all monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller ID, call forwarding, and certain Centrex features
6. CTC will not use, disclose or permit access to CPNI to identify or track Customers that call competing service providers. For example, as a local exchange carrier we do not use local service CPNI to track Customers that call local service competitors
7. Should our company provide CMRS or VoIP services, we will comply with Part 64 2005(b) as these rules relate to these services

### **Approval or Disapproval of CPNI**

1. We honor a Customer's approval or disapproval until the Customer revokes or limits such approval or disapproval
2. Other Opt-Out provisions per Part 64 2008(d) will be followed
3. If we disclose or allow access to Customers' individually identifiable CPNI to our affiliates, we will require, in order to safeguard that information, confidentiality agreements that:
  - A. Require our affiliates' use of the CPNI only for the purpose of marketing or providing the communications-related services for which the CPNI has been provided
  - B. Disallow their permitting any other party to use, allow access to, or disclose the CPNI to any other party, unless they are required to make disclosure under force of law

- C Require that they have in place appropriate protections to ensure the ongoing confidentiality of the CPNI

### **Customer Authentication for Call Detail**

1. Since the release of call detail information over the telephone presents an immediate risk to privacy, CTC is prohibited from releasing call detail information based on customer-initiated telephone contact, except under three circumstances.
  - A When a customer provides a pre-established password or provides the answer to a pre-established secret question
  - B When a customer requests that the information is sent to the customer's address of record
  - C When a representative of our company calls the telephone number of record and discloses the information
  - D Providing a password is not required for routine customer care procedures regarding service/billing disputes or questions if the customer is able to provide all of the call detail information necessary to address the customer question (i.e., telephone number called, when it was called, amount charged for the call)
2. At retail locations, we may continue to provide account access to customers who present valid photo IDs
3. In addition, CTC will provide mandatory password protection in the event that online account access is allowed. Online access based solely on a customer's readily available biographical information is prohibited. However, the Company is not required to reinitialize existing passwords for online customer accounts

### **Establishing a Password**

1. For existing customers, CTC must first authenticate the customer by either calling the account number on record or the customer presenting a valid photo id, in person at any retail location
2. For a new customer, the Company may establish a password at the time of service initiation and the customer may be authenticated at that time

### **Customer Account Authentication**

1. We will authenticate the customer for their protection and confirm the person we are speaking with is the account holder. Authentication may NOT include "readily available biographical information" or "account information" such as the following:
  - A. The social security number or the last four digits of the social security number
  - B. Mother's maiden name
  - C. City of birth
  - D. Date of birth
  - E. Home address
  - F. Account number or any component
  - G. Telephone number associated with the account
  - H. Amount of the last bill

2. We will not discuss the following account information with a spouse, child, parent, etc., unless they are authorized by the account holder. Account information may include, but is not limited to, the following.
  - A. Name
  - B. Address
  - C. Phone number
  - D. Billings or charges
  - E. Balance due or payment status
3. A maximum of four authorized contacts may be added to the account by the authorized account holder
4. All documents, notes, and printed materials with customer information will be shredded and disposed of properly. This may include, but is not limited to the following:
  - A. Social Security Number
  - B. Customer's name, address, phone number
  - C. Copy of bill or remittance slip

#### **Law Enforcement**

1. All requests for customer account or billing information will be directed to the Human Resources Manager or another member of the Human Resources Department

#### **Notice of Account Changes**

1. The Company must notify a customer immediately of account activity, such as a change to a password, online account, or address of record. Notification may be sent by email, voicemail, text message, or US Mail to the customer's address of record

#### **Notice of Unauthorized Disclosure or Breach of CPNI**

1. If there has been a breach of CPNI, the Company must provide electronic notification of the breach within seven business days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI"). (The FCC will provide a link for the reporting of breaches at [www.fcc.gov/eb/CPNI/](http://www.fcc.gov/eb/CPNI/).) In order to allow law enforcement time to conduct an investigation, the Company must wait another seven business days before notifying the affected customers of the breach (unless the USSS and FBI request that the carrier continue to postpone disclosure). However, the Company may notify customers sooner if there is a risk of immediate and irreparable harm. In addition, we must keep records of discovered breaches for at least two years

#### **Joint Venture and Independent Contractor Use of CPNI**

1. The Company must obtain opt-in consent from a customer before disclosing a customer's CPNI to a joint venture partner or an independent contractor for the marketing of communications-related services to the customer

#### **Business Customers**



1. The Company may establish contract authentication procedures for business customers that are different from residential customers, so long as those customers have a dedicated account representative and the contracts specifically address the protection of CPNI

### CPNI Compliance

1. The Company has implemented a system by which the status of a Customer's CPNI approval can be clearly established prior to the use of the CPNI
2. We have trained our personnel as to when they are and are not authorized to use CPNI
3. Any unauthorized use, sale, or otherwise disclosure of CPNI by any employee would subject the employee to disciplinary action. For the first violation, an employee will be given a warning and the violation will be noted on the employee's record. An employee will be subject to termination of employment for a second violation
4. The Company employees will sign a CPNI Policy Acknowledgement that will be placed in the employee's personnel file
5. The Company maintains a record of our own and our affiliates' sales and marketing campaigns that use Customers' CPNI. The record includes a description of each campaign, the specific CPNI that was used in the campaign, and what products and services were offered as part of the campaign. We retain these records for at least one year
6. Notification records and approval or disapproval records need to be retained for at least one year
7. The Company has established a supervisory review process regarding compliance with the CPNI rules for outbound marketing situations and we maintain compliance records for at least one year. Specifically, our sales personnel obtain supervisory approval of any proposed outbound marketing request for Customer approval of the use of CPNI
8. The Company has a corporate officer who acts as agent for the Company and signs a compliance certificate on an annual basis before March 1 of each year in EB Docket No. 06-36 stating that the officer has personal knowledge that the Company has established operating procedures adequate to ensure compliance with applicable CPNI rules. We provide a statement accompanying the certificate that explains our operating procedures and demonstrates compliance with the CPNI rules. In addition, we will include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI

COMPANY: CORDOVA TELEPHONE COOP.

Paul Kelly  
Officer

2-22-2008  
Date